REMARKS

Entry of this amendment, reconsideration, and allowance of the subject application are respectfully requested.

Claims 1-8, 11, and 22-26 stand rejected under 35 U.S.C. §102 is anticipated by U.S. Patent 6,498,843 to Cox. This rejection is respectfully traversed.

To establish that a claim is anticipated, the Examiner must point out where each and every limitation in the claim is found in a single prior art reference. *Scripps Clinic & Research Found. v. Genentec, Inc.*, 927 F.2d 1565 (Fed. Cir. 1991). Every limitation contained in the claims must be present in the reference, and if even one limitation is missing from the reference, then it does not anticipate the claim. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565 (Fed. Cir. 1986). Cox fails to satisfy this rigorous standard.

The Cox reference describes intercepting and monitoring signals in a network. Cox observes that known systems for call interception suffer from being detectable due to noise in the telephone call or requiring full control of the telephone switching office. So Cox's goal is to make the call interception and monitoring undetectable.

A call signal is intercepted and monitored based on one or more items of information such as target telephone number, a credit card number, a virtual private network number, personal identification number, a prepaid card number or a third party billing number associated with the signal (see column 2, lines 10-16). In the practical examples, only a target telephone number is mentioned. First and second sets of triggers are used for detecting a call to be intercepted, and then routing the call to a collection node 130 (See Fig. 1). When a switching node detects a signal associated with a target telephone number, the switching node identifies and executes a first predefined trigger associated with the target telephone number. That trigger

identifies a call treatment tag for routing the detected signal. The switching node then sends the identified call treatment tag to the signaling node, e.g., the signaling transfer node 150 shown in Figure 1.

Based on the identified call treatment tag, the signaling node 150 routes the signal on a provisioned route to the collection node 130. The signaling node 150 also performs normal call routing steps to route the signal to a destination node. When the set-up phase for the signal is completed, law enforcement personnel may monitor the contents of the signal at the collection node (see column 2, lines 38-60 and column 4, line 57-column 5, line 23). So Cox sets up a communication triangle for monitoring a call associated with a target telephone number. An initial address messages (IAM), in which information can be inserted, especially the tags used for routing calls is described at column 7, lines 45-50 and column 10, lines 6-9.

Claim 1 specifically recites setting up calls in a switching node "in response to the request of a virtual subscriber requesting that a call set up in accordance with a virtual subscription." Cox does not disclose virtual subscriptions or virtual subscribers. Claim 1 further recites adding "virtual subscriber identification information to the call data of a call set up by said service provision means for allowing interception of said call." Cox does not disclose virtual subscriber identification information or adding such virtual subscriber identification information to call data for allowing interception of that call. Similar features are recited in independent claims 26. Lacking these features, the anticipation rejection of claims 1 and 26 is improper and should be withdrawn.

Claims 35-49 stand rejected under 35 U.S.C. §103 as being unpatentable over Cox in view of Benash. This rejection is respectfully traversed.

The Benash reference is concerned with a public IP transport network. The goal is to provide equal access for IP transport and Internet services using a PSTN. The document is mainly concerned with arranging the IP protocol architecture in a PSTN environment. In columns 16-19, virtual numbers are mentioned, and in connection with Figure 9, it is described how a virtual telephone number is dialed and recognized by the service switching point (SSP) 520. As a consequence, the integrated services control point (ISCP) 524 is interrogated for routing instructions. Beyond this, the Benash reference does not give any specific information on virtual subscriptions.

Claim 35 explicitly recites a virtual subscriber and adding "virtual subscriber identification information to call data of the set up call." These features are lacking in both Cox and Benash. As outlined above, Cox describes detecting a call to be intercepted and then setting up a three-way communication. In the course of setting up the three-way communication, information is added to signaling messages. But there is no teaching of adding information to a call being set up for the purpose of enabling interception of the call. Nor would there be any reason to add that kind of interception information because, in Cox, the interception has already taken place. The Benash reference does not remedy these deficiencies in Cox. Benash only describes the general idea of a virtual number, similar to what is described in the introduction to the present application.

And even if the ordinarily skilled person would have considered employing virtual subscriptions (as only generally described in Benash) in the context of Cox, (for purposes of argument), the result would not add virtual subscriber identification information for the purpose of subsequent call interception. Instead, the result would be a network that performs interception according to Cox and which has nodes that can set up calls based on virtual subscriptions. There

is no teaching or suggestion in either reference of having a server that sets up a call for virtual subscribers add identification information to that call to permit subsequent interception of the call being set up.

Combining Cox and Benash produces a system in which a switching node of Cox interrogates the signaling node for information on routing the virtual call. So what reason is there to add any information identifying the virtual subscriber? Call interception has already taken place in Cox. Consequently, there is no point in adding information identifying a virtual subscriber.

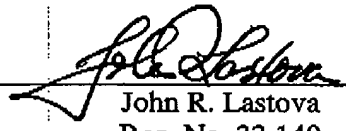
Claims 9, 10, 12-21, and 27-34 stand rejected based on Cox and U.S. 6,370,241 to Clark. This rejection is traversed.

The service provision means of claim 27 provides a monitoring agency continuous access to user data of virtual subscribers or performs a user data change interception operation in response to a virtual subscriber changing his data. With respect to claim 27, the Examiner refers to his rejection of claims 1, 12, 16, and 17 (see page 11 of the Official Action). On page 10, the Examiner argues against claim 17 by stating that Cox teaches sensing and intercepting based on a user changing data when a change of service is requested. The Examiner relies on column 6, lines 28-32 of Cox. But this cited passage from Cox only relates to detecting changes associated with the status of a detected signal, i.e., changes relating to an ongoing call. This has nothing to do with detecting changes in records associated with a virtual subscriber. Clark does not remedy the shortcomings of Cox.

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
John R. Lastova
Reg. No. 33,149

JRL:sd
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100